utimaco® safeware

SafeGuard Easy

Document Version:	1.04.00
Document Type:	FIPS 140-2 Level 1 Security Policy
Project Id:	
File Name:	SGE-Fips140-SecurityPolicy-1-04-00
Author(s):	Roland Reinl
Office / Company:	Utimaco Safeware AG

Abstract: This document contains the non-proprietary Security Policy for the validation of SafeGuard Easy Version 4.20 according to FIPS 140-2 Level 1.

Table Of Contents

1 Document Information

1.1 Owner / Master Location

Owner of this document is Christian Tobias (CTO).

The location of the master copy is CTO user area, network Utimaco Oberursel at SGE-Fips140-SecurityPolicy-1-04-00

1.2 Change History

Version	*Author*	*Date (finished)*	*Description*
1.00.00	RRE	22.11.2005	First Version
1.01.00	CTO	08.03.2006	Algorithm Certificate Numbers added
1.02.00	CTO	20.03.2006	Editorial Changes
1.03.00	RRE	29.06.2006	Sections 3.2 and 3.5 amended, Editorial Changes
1.04.00	CTO	08.09.2006	Section 3.5 updated

1.3 Distribution & Approval History

Version	*Distributed to / approved by*	*Date distributed*	*Date approved*
1.00.00	Domus ITSL / CTO	06.12.2005	06.12.2005
1.01.00	Domus ITSL / CTO	08.03.2006	08.03.2006
1.02.00	Domus ITSL / CTO	20.03.2006	20.03.2006
1.03.00	Domus ITSL / CTO	04.07.2006	04.07.2006
1.04.00	Domus ITSL / CTO	08.09.2006	08.09.2006

1.4 Assumptions made herein

2 Introduction

2.1 Purpose

This document provides the Cryptographic Module Security Policy for a validation according to the standard of FIPS 140-2 for the software product “SafeGuard Easy Version 4.20”.

The manufacturer and the vendor of the product is Utimaco Safeware AG.

The SafeGuard Easy product is claimed to meet the overall requirements applicable to Level 1 security for FIPS 140-2.

This security policy describes the definition and boundaries of the SafeGuard Easy Cryptographic Module, its compliance to the security requirements of FIPS 140-2 and how to use SafeGuard Easy in a secure FIPS 140-2 mode.

2.2 References

This document contains only information related to the FIPS 140-2 compliant operation of SafeGuard Easy. Further information about the SafeGuard Easy product or information about other products offered by Utimaco Safeware AG is available at the Utimaco website: http://www.utimaco.com.

Information about the FIPS 140-2 standard and the Cryptographic Module Validation Program is available at the following website:

http://csrc.nist.gov/cryptval

2.3 Document Organisation

For the validation according to FIPS 140-2 the following documents are delivered by the manufacturer:

- Security Policy (this document)
  It contains non-proprietary information about the cryptographic module and its intended method of use.
  This document may be made open to public.
- Vendor Evidence Document
  It contains additional information, how the cryptographic module meets the security requirements of FIPS 140-2. This information may partly consist of references to other documents.
  This document contains information proprietary to Utimaco Safeware AG and shall not be published.

- Additional documentation
  Other documents, which contain information required for the validation of the cryptographic module. These documents are referenced by the Security Policy or the Vendor Evidence Document.
  These documents may contain information proprietary to Utimaco Safeware AG and shall not be published.

3 SafeGuard Easy Cryptographic Module

3.1 Overview

SafeGuard Easy (SGE) is a software product designed to protect user data on all types of Personal Computers (PCs) running Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows 2000 Server or Microsoft Windows 2003 Server as operating system. SafeGuard Easy is installed on a PC to prevent unauthorised access to user data stored on hard disk partitions. In this context, user data means all files on hard disk partitions, i.e. data files, program files and even files of the operating system. The protection of the user data stored on hard disk partitions is realised by encryption. Encryption is done on sector level - not on file level. This provides the advantage of being independent from the behaviour of application programs and processing files difficult to handle, like temporary file areas or paging files of the operating system.

Additionally, data stored on floppy disks and other removable devices (e.g. MO drives, ZIP drives) may also be protected by symmetric encryption.

SafeGuard Easy is installed from CD-ROM. The installation program together with the administration program installs the system kernel of SGE on the hard disk, adds some drivers to the operating system, changes the master boot record, and initially encrypts the hard disk partitions. After having installed SGE and completed the hard disk encryption, the PC is protected.

3.2 Cryptographic Module Definition

The SafeGuard Easy Cryptographic Module is defined as a multi-chip standalone module in the terms of FIPS 140-2.

The following components of the delivered product are parts of the tested cryptographic module:

- The Real Mode Encryption Handler of SafeGuard Easy
- The Protected Mode Crypto Drivers of SafeGuard Easy

The following figure depicts the cryptographic module and its environment.

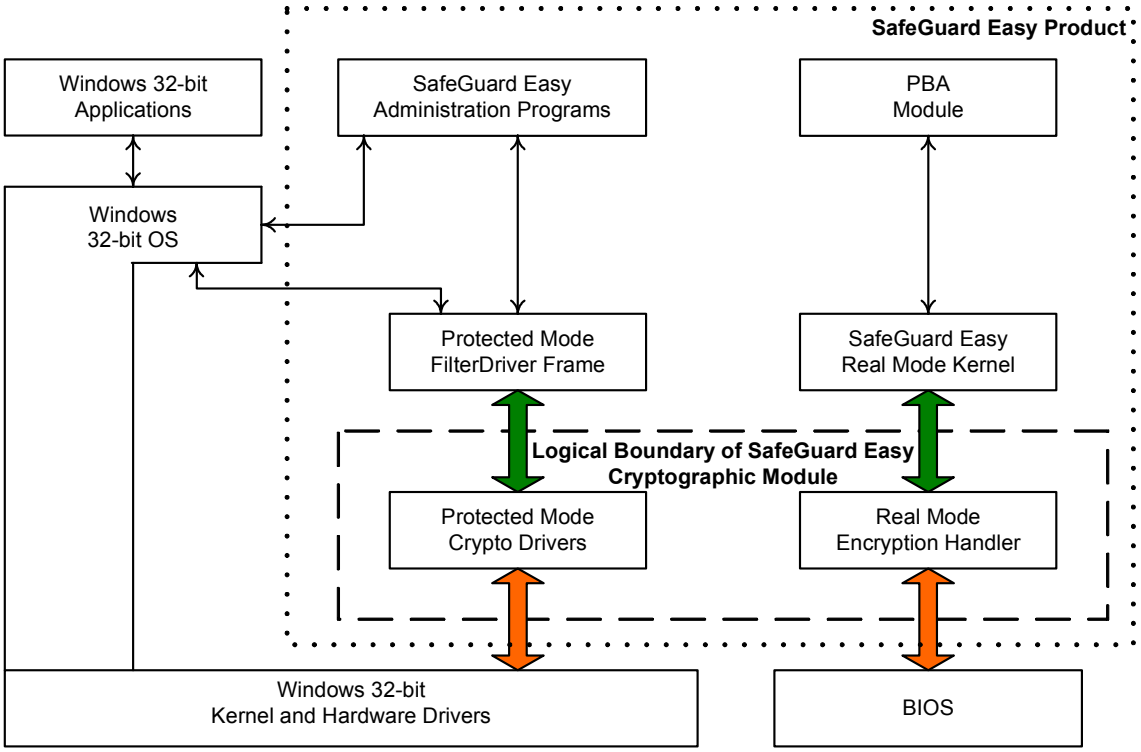

Figure 1: Cryptographic Module Scheme

Description of Figure 1:

The dashed line defines the logical boundary of the SafeGuard Easy Cryptographic Module. The colored arrays show the encryption/decryption services of the cryptographic module: a red arrow means ciphertext data, a green arrow means plaintext data.

The cryptographic module is a pure software module and is running on the following target hardware device.

- an industry standard PC or notebook equipped with a microprocessor with IA32 architecture running one of the following Windows 32-bit operating systems: Windows 2000, Windows XP, Windows 2000 Server or Windows 2003 Server; the code of the module is executed on the built-in microprocessor.

The following figure simplified shows the interaction between SafeGuard Easy, the Windows operating system and any application program while the cryptographic module is in operational state:

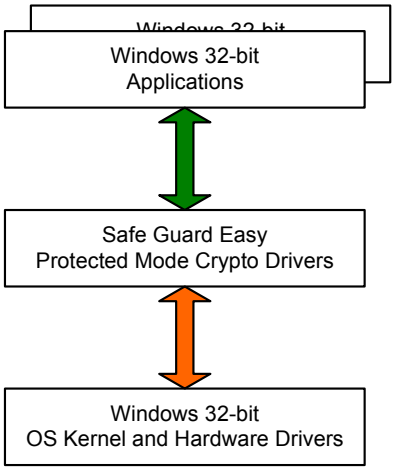

Figure 2: Interaction between Cryptographic Module and Environment

Description of Figure 2:

Like in figure 1 the colored arrays show the encryption/decryption services of the cryptographic module: the red arrow means ciphertext data, the green arrow means plaintext data.

SafeGuard Easy Cryptographic Module provides the following FIPS-approved algorithms:

Algorithm	Purpose	FIPS standard	Certificate No.
AES-128 and AES-256	symmetric encryption with 128 bit rsp. 256 bit key length	FIPS 197	#364
Triple-DES	symmetric encryption with 192 bit key length	FIPS 46-3	#416
SHA-256	secure hash	FIPS 180-2	#438
HMAC-SHA-256	integrity check	FIPS 198	#162

Table 1: FIPS-Approved Algorithms Provided by SafeGuard Easy Cryptographic Module

SafeGuard Easy Cryptographic Module also supports the following Non-FIPS-approved algorithms:

- Rijndael-256
- IDEA
- DES, not compliant with FIPS 140-2
- Blowfish
- Stealth-40
- XOR

3.3 Interfaces

The physical boundary of the SafeGuard Easy Cryptographic Module is the physical boundary of the PC, on which SafeGuard Easy is running:

The standard PC or notebook with its case and external interfaces for keyboard, HIDs (e.g. mouse), display, data storage devices (e.g. hard disk, CD-ROM), network ports, USB, serial and parallel interface ports etc.

The following figure shows the hardware block diagram including the physical boundary and the data flow within the physical boundary of the cryptographic module:

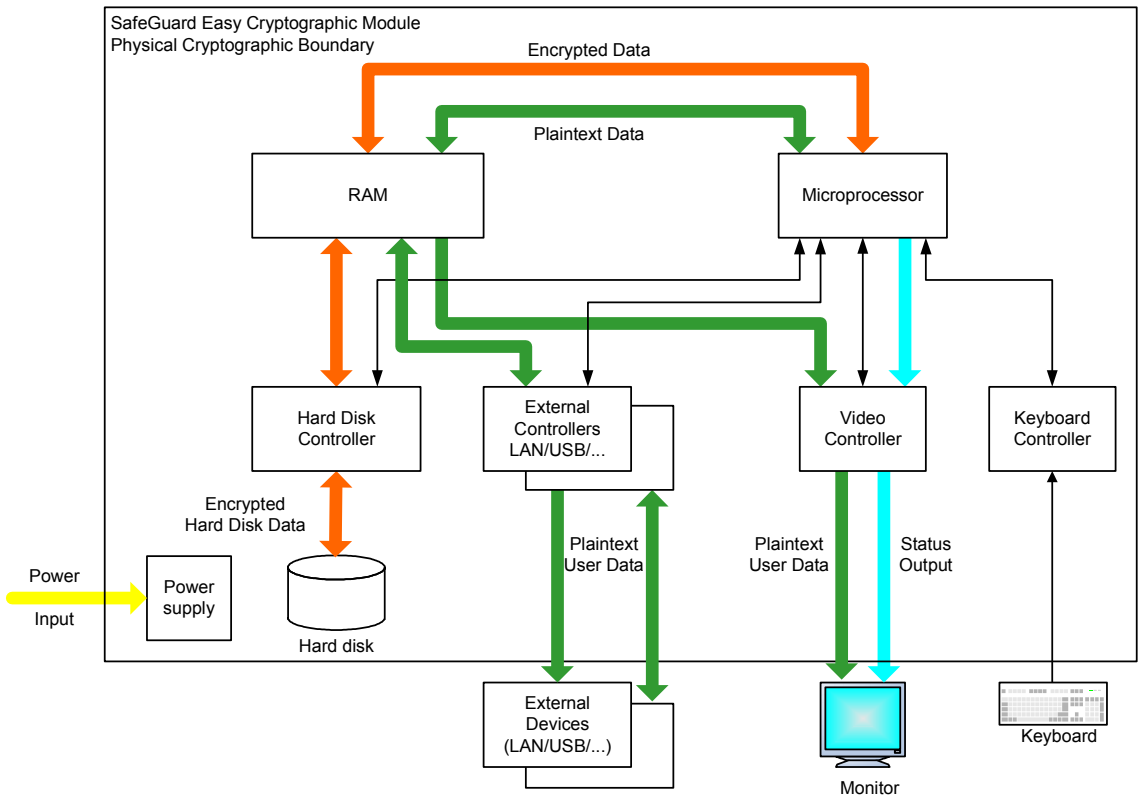

Figure 3: Hardware Block Diagram of SafeGuard Easy Cryptographic Module

Description of Figure 3:

The colored arrays show the data flow within the cryptographic module: the red arrows mean ciphertext data, the green arrows mean plaintext data, the blue arrows represent status output, the yellow arrow represents the power interface and the black thin arrows represent internal commands of the PC.

The logical interfaces of the SafeGuard Easy Cryptographic Module are defined as follows:

- The API function calls of the Real Mode Encryption Handler,
- The API function calls of the Protected Mode Crypto Drivers.

Data input are certain API function calls and their parameters. The parameters may directly contain input data or may be pointer referencing memory data buffers with input data.

Data output are parameters of certain API function calls. The parameters are pointer referencing memory data buffers where output data shall be stored.

Control input are certain API functions calls for initialization and status check.

Status output are the return values of the included API function calls.

The logical interfaces, physical interfaces and cryptographic module interfaces can be mapped like shown in the table below:

Logical Interface (FIPS 140-2)	Module Interface	Physical Port
Data Input Interface	API function calls containing parameters with input data or pointers to input data buffers	Keyboard, HIDs, data storage devices, external ports (network, USB, serial etc.)
Data Output Interface	Parameters of API function calls pointing to output data buffers	Display, data storage devices, external ports (network, USB, serial etc.)
Control Input Interface	API function calls provided for initialization and control of the module	data storage devices, external ports (network, USB, serial etc.)
Status Output Interface	Return values of certain API function calls	Display, data storage devices, external ports (network, USB, serial etc.)
Power Interface	not applicable	PC/power interface

Table 2: Interfaces of SafeGuard Easy Cryptographic Module

3.4 Roles and Services

The SafeGuard Easy security policy supports two roles:

- Crypto Officer role and
- User role

All services are implicitly assumed by both the Crypto Officer and User roles. Any user, who is operating a PC with disk encryption enabled by SafeGuard Easy is assumed to hold the User role. This role allows to use the cryptographic operations as provided by SafeGuard Easy.

The Crypto Officer role is applied to the system administrator, who is installing SafeGuard Easy containing the SafeGuard Easy Cryptographic Module on a target system and who is providing the keys used for hard disk encryption during the installation process.

There is no specific authentication mechanism provided by the SafeGuard Easy Cryptographic Module neither for the User role nor for the Crypto Officer role.

The SafeGuard Easy Cryptographic Module provides the following services:

- Symmetric data encryption (AES-128, AES-256 and Triple-DES)
- Symmetric data decryption (AES-128, AES-256 and Triple-DES)
- Hash generation (SHA-256)
- MAC generation (HMAC-SHA-256)

The services are provided to the User role as well as to the Crypto Officer (CO) role as specified in the table below.

Role	Service	Affected Keys and CSPs	Access
CO	Input Key	AES or Triple DES Key	Execute
	Run Self-Tests	HMAC Key	Execute
User	Encrypt/Decrypt	AES or Triple DES Key	Execute
	HMAC	HMAC Key	Execute
	Run Self-Tests	HMAC Key	Execute
	Show Status	None	Read

Table 3: Roles and Services of SafeGuard Easy Cryptographic Module

3.5 Key Management

SafeGuard Easy Cryptographic Module uses the following keys:

- Symmetric encryption keys for AES and Triple-DES,
- Key for generating HMAC-SHA-256

The symmetric encryption keys are used for symmetric encryption by the AES and Triple-DES algorithm. The key length depends on the selected algorithm.

The key for HMAC-SHA-256 is used for the calculation of the HMAC verifying the software integrity.

The module does not implement key establishment. Keys are installed as part of the setup and initialization process of SafeGuard Easy. Once installed, keys are never output from the module. As this is a disk encryption product, all data and keys within the physical boundary are encrypted on the hard disk when the PC is powered off. The key encryption key however is a derived encryption key from a password and from a FIPS 140-2 validation

perspective, is considered stored in plaintext. Keys are temporarily stored in NVRAM when the PC and OS have been initialized and the hard disk is ready to be decrypted.

The keys are stored in RAM until the operating system is shut down or the PC is powered off. At that point, all encryption keys initialized into memory are destroyed.

The SafeGuard Cryptographic Module can destroy all keys by formatting the hard drive.

SafeGuard Easy Cryptographic Module also supports the following Non-FIPS-approved algorithms which cannot be chosen in FIPS mode: Rijndael-256, IDEA, DES, Blowfish, Stealth-40 and XOR.

3.6 Physical Security

As the SafeGuard Easy Cryptographic Module is a pure software module, there is no physical security requirement to be fulfilled by the module itself.

However, the Crypto Officer shall ensure the physical security of the computer systems, where SafeGuard Easy has been installed and is operational.

3.7 Operational Environment

The SafeGuard Easy Cryptographic Module performs an integrity test at startup using HMAC-SHA-256.

The module was tested on Windows 2000 SP4, Windows XP SP2, Windows 2000 Server SP4 and Windows 2003 Server SP1.

3.8 Self Tests

The SafeGuard Easy Cryptographic Library performs the following tests at initialization:

- Software integrity test (HMAC-SHA-256)
- Triple-DES Known Answer Test
- AES Known Answer Test

The library also has the ability to run self-tests on demand by executing the “runselftest()”

3.9 Mitigation of Other Attacks

The module does not contain security mechanisms to mitigate other attacks outside the security requirements of FIPS 140-2.

4 Secure Operation

4.1 SafeGuard Easy Installation

The following requirements shall be followed by the Crypto Officer during installation of SafeGuard Easy:

- The SafeGuard Easy Cryptographic Module is installed as part of the SafeGuard Easy Disk Encryption product.
- In FIPS mode only Triple-DES or AES can be selected as the symmetric disk encryption algorithm; AES-256 is the default setting.
- The operator must verify that the FIPS Mode icon in the task bar is visible and is shown in green color in order to verify that the module is in FIPS Approved Mode of operation. If the FIPS Mode icon is not visible or shown in red color, the module is not in FIPS Mode.

4.2 FIPS Approved Mode of Operation

The following requirements shall be followed during the operation of the SafeGuard Easy Cryptographic Module:

- Only FIPS approved algorithms (Triple DES or AES symmetric encryption) may be used in FIPS mode.
- The operating system must be configured in single user mode of operation.
- Keys are never input or output from the physical cryptographic boundary.
- The operator must verify that the FIPS Mode icon in the task bar is visible and is shown in green color in order to verify that the module is in FIPS Approved Mode of operation. If the FIPS Mode icon is not visible or shown in red color, the module is not in FIPS Mode.

5 Terms and Definitions

5.1 Abbreviations

CO	Crypto Officer
DLL	Dynamically linkable library
FIPS	Federal Information Processing Standards
SGE	SafeGuard Easy
HID	Human Interface Device
OS	Operating System
PC	Personal Computer
PBA	Pre Boot Authentication

6 References

[FIPS 46-3] "FIPS PUB 46-3, Data Encryption Standard (DES)", National Institute of Standards and Technology, October 25, 1999

[FIPS 140-2] "FIPS PUB 140-2, Security Requirements for Cryptographic Modules", National Institute of Standards and Technology, May 25, 2001

[FIPS 180-2] "FIPS PUB 180-2, Secure Hash Standard with Change Notice 1", National Institute of Standards and Technology, February 25, 2004

[FIPS 197] "FIPS PUB 197, Advanced Encryption Standard (AES)", National Institute of Standards and Technology, November 26, 2001

[SGE-VED] "SafeGuard Easy, FIPS 140-2 Level 1 Vendor Evidence Documentation", Version 1.00, Utimaco Safeware AG, November 2005